MAYER | BROWN

October 16, 2019

Cybersecurity & Data Privacy

Strategic Thinking and Practical Legal Advice

US and UK Sign Historic Bilateral Data Access Agreement

On October 7, 2019, the United States and United Kingdom released the text of a bilateral data access agreement that would permit law enforcement authorities in one country to make direct requests to communications service providers based in the other country for electronic evidence related to serious crimes, including terrorism. This would allow such companies to provide the requested information without going through the existing mutual legal assistance process.

The UK-US Bilateral Data Access Agreement (the "Agreement") would be a legally binding executive agreement that is intended to advance public safety and security. The Agreement will provide authorities in both nations with an efficient means for obtaining electronic data relating to "serious crimes"—defined in the Agreement as "offenses punishable by a maximum term of imprisonment of at least three years." The Agreement—the first executive agreement negotiated under the Clarifying Lawful Overseas Use of Data ("CLOUD") Act—is also negotiated pursuant to authorities set out in the UK's Investigatory Powers Act 2016 and Crime (Overseas Production Orders) Act 2019.

Additional privacy safeguards built into the Agreement are designed to ensure both US and UK authorities comply with certain privacy and civil liberty expectations—a prerequisite to entering into an executive agreement under the CLOUD Act. Ultimately, these prerequisites may prove challenging for some countries attempting to negotiate similar bilateral executive agreements with the United States.

The Current Process

Due to certain barriers in US law, access by UK authorities to content held by US communications service providers can take years. As we explained last year, the United States' Stored Communications Act[1] has been interpreted to prohibit US communications service providers from providing certain requested data without a warrant, subpoena or court order. Thus, foreign law enforcement authorities seeking to obtain electronic data from US communications service providers must do so under a Mutual Legal Assistance Treaty ("MLAT"). Requests for mutual legal assistance are a form of cooperation between countries for the purpose of collecting and exchanging information. This cross-border data-sharing mechanism allows law enforcement authorities in the one country to seek the assistance of foreign partners who can obtain the data. The foreign partner reviews a request under its own legal standards and may seek a court order under its law to obtain the data. If the order is granted, the foreign government obtains the data and transmits it to the requesting government. The United States and United Kingdom have such an agreement in place; however, an increase in the

number of requests and the cumbersome administrative legal process associated with MLAT requests have led to significant wait times of between six months to two years.

The CLOUD Act

Enacted in March 2018, the CLOUD Act grants certain countries the ability to enter into executive agreements with the United States to obtain access to electronic evidence, wherever it happens to be located, in order to investigate serious crime and terrorism. Before entering into an executive agreement under the Act, the US Attorney General must certify to the US Congress that the partner country has in its laws, and implements in practice, robust substantive and procedural protections for privacy and civil liberties. The US Attorney General considers such factors as whether the partner country has:

- adequate substantive and procedural laws on cybercrime and electronic evidence, such as those enumerated in the Convention on Cybercrime, E.T.S. No.185 (also known as the Budapest Convention);
- respect for the rule of law and principles of nondiscrimination;
- adherence to applicable international human rights obligations;
- clear legal mandates and procedures governing the collection, retention, use and sharing of electronic data;
- mechanisms for accountability and transparency regarding the collection and use of electronic data; and
- a demonstrated commitment to the free flow of information and a global Internet.

Once certified, the Attorney General provides notice of its determination and a copy of the executive agreement to Congress. Congress then has 180 days from the date notice is issued to issue a joint resolution of disapproval, rejecting the proffered executive agreement. If no such resolution is issued, the executive agreement enters into force as a matter of US domestic law.

In order to ensure partner countries comply with US privacy and civil liberty expectations, the Act sets out a number of restrictions for parties seeking to request data. Specifically, orders seeking data:

- must be lawfully obtained under the domestic system of the requesting country;
- must target specific individuals or accounts;
- must have a reasonable justification based on articulable and credible facts; particularity, legality and severity;
- must be subject to review or oversight by an independent authority;
- may not target US persons or persons in the United States; and
- may not infringe on freedom of speech.

Further, bulk data collection is not permitted and requesting parties may only obtain information relating to the prevention, detection, investigation or prosecution of serious crime, including terrorism.

Though the CLOUD Act provides a way for authorities to avoid the lengthy MLAT process, requests for mutual legal assistance may still be made by authorities whose requests are not covered by the CLOUD Act.

The Crime (Overseas Production Orders) Act

The Crime (Overseas Production Orders) Act became law within the United Kingdom on February 12, 2019, and, similarly to CLOUD in the United States, paved the way for the United Kingdom to enter into bilateral data access agreements with other countries. Amongst other provisions, the Act ensures that any future agreements will incorporate the following conditions:

- robust judicial oversight;

- protections for legally privileged material and journalistic data; and
- assurances that UK data will not be used in cases that could result in the death penalty.

The Crime (Overseas Production Orders) Act supplements the Investigatory Powers Act 2016, which provides the basic framework that governs the use of investigatory powers by UK law enforcement agencies.

The Agreement

The Agreement incorporates the restrictions and preconditions outlined by the CLOUD Act (i.e., requests must be targeted to specific individuals or accounts, requests may not target US persons or persons in the United States, etc.). There are, however, additional safeguards included in the Agreement beyond the CLOUD Act's requirements. These include:

- **Designated Authorities.** Under the Agreement, orders must be reviewed and certified (in writing) by a designated authority. In the United States, this authority will be designated by the Attorney General. In the United Kingdom, this authority will be designated by the Secretary of State for the Home Office.
- **Objections and Veto Power.** The Agreement affords communications services providers the opportunity to raise objections to an order with the designated authority that issued the order. The provider's objections may be escalated and raised with their own designated authority if necessary, and the governments must work together to determine an outcome. Notably, the provider's designated authority has veto power and may ultimately block execution of the order. The United Kingdom also has the power to veto the use of any evidence obtained for cases in which the death penalty is sought, and the United States may veto the use of any evidence in cases that raise free speech concerns.
- **Notification.** When law enforcement authorities in the United Kingdom request the data of an individual believed to be outside of the United Kingdom, or law enforcement authorities in the United States request the data of an individual believed to be outside of the United States, the requesting government must notify the government of the third country where the person is located. Such notification is not required if doing so would be detrimental to the investigation, operational or national security, or human rights.
- **Minimization.** The Agreement outlines steps the UK government must take in order to minimize the acquisition, retention and dissemination of any data that is acquired pursuant to an order subject to the Agreement and which concerns US persons.
- **Reciprocity.** Under the CLOUD Act, the United Kingdom may not target the data of US individuals or individuals living in the United States. The Agreement includes a similar provision regarding the United States' obligations. Specifically, the United States may not target the data of UK citizens within the United Kingdom; however, once the individuals leave the United Kingdom, this restriction no longer applies.
- **Reporting Requirements.** Each party to the Agreement must review the other party's compliance with the terms of the Agreement on an annual basis. The Agreement further mandates that both countries must issue an annual report reflecting aggregate data concerning the use of the agreement.

Officials expect that the Agreement will hasten investigations into serious crimes and terrorist threats. Unlike the MLAT, authorities can go directly to communications service providers—with proper authorization—and demand electronic data. The streamlined and more direct process is expected to help reduce the request time from months and years to days or weeks.

The US Congress has 180 days to review the text, after which, pending no objections, the Agreement will enter into force. The UK Parliament must ratify the Agreement and then designate it as an international agreement under the Investigatory Powers Act 2016 and Crime (Overseas Production Orders) Act 2019. The Agreement will therefore not enter into force until the necessary legislative steps in each country have been completed.

Domestic Laws and Privacy Concerns

US authorities have stressed that due to the stringent procedural and substantive standards to enter into executive agreements under the CLOUD Act, certain countries will need to increase their privacy protections to be eligible to engage with the United States under the Act.

Of particular concern to communications service providers is whether the contents of encrypted communications stored on their networks must be disclosed under the Agreement. While the Agreement does not address whether companies may encrypt data on their platforms, the CLOUD Act expressly provides that executive agreements must be "encryption neutral," neither requiring decryption nor foreclosing governments from ordering decryption to the extent authorized by their laws. As such, there remains uncertainty as to how the two governments will interpret requests for encrypted communications under the Agreement.

Future Agreements

Negotiations between the United States and Australia of a bilateral agreement under the CLOUD Act began this week. Mirroring the agreement between the United States and United Kingdom, if signed, this agreement would permit communications service providers in the United States and Australia to respond to orders from the other country without violating disclosure and data transfer restrictions.[2]

For more information about the topics raised in this Legal Update please contact any of the following lawyers:

Rajesh De
rde@mayerbrown.com
+1 202 263 3366

Mark Prinsley
mprinsley@mayerbrown.com
+44 20 3130 3900

David Simon
dsimon@mayerbrown.com
+1 202 263 3388

Kendall Burman
kburman@mayerbrown.com
+1 202 263 3210

Veronica Glick
vglick@mayerbrown.com
+1 202 263 3389

Joshua Silverstein
jmsilverstein@mayerbrown.com
+1 202 263 3208

Amber Thomson
athomson@mayerbrown.com
+1 202 263 3456

Endnotes

[1] 18 U.S.C. § 2701 et seq.

[2] Concerns from the US House of Representatives that Australia's "Assistance and Access" laws may not conform to the CLOUD Act have been raised with Australia's Home Affairs Minister. As discussed in this Legal Update, an agreement under the CLOUD Act can only be approved if the United States determines that Australia has substantive and procedural protections for privacy and civil liberties and does not include requirements for decryption of user data. The Assistance and Access laws grant authorities the power to obtain encrypted communications of criminal suspects from communications service providers.